AUTOMATED TELLER MACHINES AND ELECTRONIC FUNDS TRANSFERS AT POINT OF SALE: SELECTED LEGAL ISSUES[1]

The advent of computer technology has made banking more convenient to the consumer. As in the case of many other financial centres in the world, computer technology has been introduced in Singapore. The government is encouraging the use of electronic transfer of funds as it cuts back on paperwork and is perceived to be more productive. Such technology, as it relates to consumer banking, finds expression in the form of automated teller machines (ATMs), electronic funds transfer at the point of sale (EFTPOS), GIRO systems and home telephone banking. This article discusses some legal issues arising from the use of ATMs and EFTPOS and approaches them from the viewpoint of the bank and its cardholder.

I. INTRODUCTION

THE drive to create a cashless society in Singapore has gained momentum. In 1984, the Committee to Minimise Cash Transactions (COMMICT) was formed with the objective of making cashless transactions a way of life for Singaporeans by 1987. The Committee has substantially achieved this objective and was dissolved on 19 January 1986. Some features of this cashless, or, more accurately, less cash phenomenon which have some bearing on consumers are automated teller machines (hereinafter referred to as "ATMs"), credit and charge cards, payment of salaries through bank accounts (Inter-bank GIRO),[2] the gradual phasing out of Multi-Revenue Collection

[1] A paper on the same topic was delivered at a seminar on "Cashless Society and the Consumer" organised by the Consumer Association of Singapore (hereinafter referred to as "CASE") on 26 January 1986. This article is essentially an elaboration of points raised in that paper. Arising from the seminar, a Working Committee on Electronic Banking comprising representatives from CASE, the Association of Banks in Singapore, the Monetary Authority of Singapore, Ministry of Finance, Network for Electronic Transfers (S) Pte. Ltd. (NETS), Post Office Savings Bank, Attorney-General's Chambers and the Singapore Retail Merchants' Association was formed in April 1986. The writer was invited to sit on the Committee by CASE. Subsequently, the writer joined CASE'S Central Committee. However, the writer wishes to make clear that the views expressed in this paper are those of the writer alone and do not represent the views of the Working Committee or CASE'S Central Committee even though some of the views expressed may be similar. The Working Committee submitted its report, titled "Consumer Use of Electronic Funds Transfer Systems", in May 1987. It was favourably received by all concerned, including the Association of Banks in Singapore.

[2] As of 11 August 1986, the "Big Four" banks in Singapore, (Development Bank of Singapore (DBS), Overseas Chinese Banking Corporation (OCBC), United Overseas Bank (UOB) and Overseas Union Bank (OUB)), together with the government-backed Post Office Savings Bank (POSB) had a total of 531 ATMs. As of 1 January 1987, the number of ATMs stood at about 638, and about 1.7 million ATM cards had been issued to consumers. With approximately 200 ATMs per million people, Singapore ranks third in the world. (See *Straits Times,* 11 August 1986). As for charge and credit cards, over the past ten years, an estimated 285,000 cards have been issued by the five top card-issuers, that is Diners, American Express, Carte Blanche, Visa and Mastercard. (See Consumer, publication of CASE, June 1986 at p. 6) By early 1986, 630,000 workers or 51% of the salaried workforce in Singapore had cashless paydays. (See paper presented by Mr. Wee Tew Lim, Director of Corporate Services, POSB at CASE seminar, *supra.,* n(1).).

System (MRCS) counters,[3] and the introduction by Telecoms of Phone Cards and home telephone banking.[4] The latest addition to this growing list of innovations is the process of transferring funds by the use of computers at the point of sale called "EFTPOS" (electronic funds transfer at point of sale).[5]

This move into the computer age presents many exciting possibilities. It also presents many challenges and problems: not least of these problems are those that surface in the legal realm. Often, it is the case that technological advances precede a search for legal answers to fit novel situations. In computer banking, as in other innovative areas of banking and finance, some legal issues await definitive answers. The commercial practice of computer banking has moved ahead of the law.[6] The law can fill this gap by legislation, by self-governing codes or by the creative interpretation and application of existing legal principles. The writer does not intend to deal with the whole range of computer-related transactions where funds are transferred by electronic means. Rather, the focus will be on ATMs and EFTPOS, two processes which impinge quite substantially on the lifestyle of consumers. In particular, users' (hereinafter referred to as "cardholders") rights vis-a-vis banks in these transactions will be examined. I would preface my comments set out below by saying that the views expressed therein are strictly personal ones.[7]

Principles of law that may have application in ATMs and EFTPOS transactions traverse the neat pigeon holes with which law students are familiar. They arise, *inter alia,* in the law of contract, the law of torts as in the areas of negligence and defamation, criminal law, the law of intellectual property, the law governing cheques and the law applicable to a bank-customer relationship. The discussion below will throw up some of these principles. Where applicable, comparisons will be made with the position in other countries, in particular the United States. Also, mention will be made of the *Draft Legal Guide On*

3 When COMMICT was first formed, only about 450,000 bills or 10% of all bills originating from government departments and statutory boards were paid monthly through the GIRO system operated by the banks. As at the end of 1985, POSB alone handled 854,129 GIRO transactions. (See paper presented by Mr. Wee Tew Lim, Director of Corporate Services, POSB at CASE seminar, *supra,* note 1) As of 1 January 1987, the estimated number of GIRO standing orders for payment by bank transfer was about 1.6 million.

4 Home telephone banking was first introduced in 1982, by one bank initially and then followed by other banks. Various banking transactions including checking on current account balances, paying bills of designated customers, transferring funds from one account to another and requesting new cheque books can be carried out by customers.

5 The possibility of introducing EFTPOS in Singapore was seriously considered in early 1985 by a steering committee comprising representatives from POSB and the "Big Four" banks. A feasibility study and subsequently a pilot project were carried out which proved successful. Presently, EFTPOS facility is available, as an additional feature, to the 1.5 million cardholders of POSB and the "Big Four" banks and their subsidiaries through the auspices of a company formed in 1985 by the banks called Network for Electronic Transfers (S) Pte. Ltd. (NETS). As of 1 January 1987, about 578 terminals have been installed at about 242 retail outlets.

6 See, for example, Ellinger, "The giro system and electronic transfer of funds" (1986) L. M. C. L. 178, at p. 195 where he writes, "It is difficult to define the legal nature of money transfer orders. Despite the popularity which operations of this type have attained in the course of the last decade there remains a dearth of case-law in point." Other areas of commercial law where this phenomenon is present would include leasing, factoring of account receivables, counter-trade and securities "forward contracts".

7 *Supra,* note 1.

Electronic Funds Transfer prepared by the United Nations Commission on International Trade Law.[8]

II. Legal Issues Arising

The following issues will be examined:

1. Who should bear the loss of an unauthorised withdrawal resulting from the fraud of a third party? A related question would be: who should bear the burden of proving that such fraud has indeed occurred and that the cardholder was/was not at fault.
2. What should be the required standard of care of a cardholder with respect to the safekeeping of his card and maintaining confidentiality of his personal identification number (hereinafter referred to as "PIN")?
3. What is the legal liability of the bank if it fails to make payment when instructed to do so by the cardholder?
4. Is there a need for legislation?
5. Is there a need to revise some of the current terms in the bank-cardholder contract?

(a) *Who should bear the loss arising from the debiting of a cardholder's account which he claims he has not effected and knows nothing about (hereinafter referred to as an "unexplained debit")? Who should bear the burden of showing how the unexplained debit has occurred?*

In relation to the volume of electronic funds transfers carried out, the number of reported unexplained debits has been miniscule.[9] Nevertheless, such an incident is distressing to the affected consumer. The amount involved in absolute terms may not be large, but it may be so relative to the means of the affected consumer. Moreover, if the loss for such unexplained debits invariably falls on the consumer, consumer confidence in the system may be jeopardised. It is therefore necessary that this situation be examined.

Under the present position, there would seem to be a presumption of fault on the part of the cardholder whenever there is an unexplained debit. Usually, by the terms of the bank-cardholder agreement, the bank's records are deemed to be correct and are therefore binding. The cardholder has to bear the full loss. However, it is noted that an unexplained debit may result from default by either cardholder or

[8] The United Nations Commission at its fifteenth session in 1982 decided that the Secretariat should begin the preparation of a legal guide on electronic funds transfers in cooperation with the UNCITRAL Study Group on International Payments. Several chapters of the draft legal guide were submitted to the Commission at its seventeenth session in 1984 for general observation and two additional chapters were submitted at its eighteenth session in 1985. Copies of the guide were then sent to governments and interested international organisations for comment. Eight governments and seven international intergovernmental or non-governmental organisations responded. The unanimous response was that the draft Legal Guide was a useful tool for legislators and lawyers preparing the rules governing particular funds transfer systems. (See *Official Records of the General Assembly, Thirty seventh Session, Supplement No. 17* (A/37/17) paras. 73 and 92; A/CN. 9/250 and Add. 1 to 4; A/CN. 9/266 and Add. 1 and 2 and A/CN. 9/278).

[9] For example, in the period of January to September 1985, the total volume of ATM transactions was 7.5 million whilst the number of reported complaints was 81.

bank.[10] For example, the cardholder may be at fault for enabling a third party such as a friend, colleague or family member to obtain possession of his card together with knowledge of his PIN thereby making it possible for such third party to effect an unauthorised withdrawal. On the other hand, the cardholder may be totally faultless, as when the unexplained debit results from bank default or computer malfunction. In such a situation, the cardholder will find it immensely difficult to prove that bank default or computer malfunction has occurred. How can he prove any of the following to be the reason for the debit: human error, fraud or failure to comply with safety procedures on the part of a bank employee, inadequate controls maintained by the bank, inadequate system design or systems failure? It is therefore possible that a cardholder will end up without recourse if he is a victim of any of these instances of bank default or computer malfunction. In practice, the banks, by reviewing their records, will be able to ascertain whether any of the above has indeed taken place. If it has, they will credit the cardholder's account accordingly. However, for avoidance of doubt and to inject the element of good faith and trust in the bank-customer relationship, it is suggested that banks should, in the agreement, state clearly that whenever a report of an unexplained debit is lodged, they will forthwith and in good faith check if bank default or computer malfunction has occurred.

If the bank concludes that there has been no bank default or computer malfunction, the cardholder will find himself saddled with an extremely unenviable task. How can he show that he has not been at fault for the unauthorised withdrawals? In practice, the bank will conduct an investigation into the circumstances surrounding the loss. This often takes the form of intensive questioning of the cardholder on his actions in relation to the safekeeping of his card and the maintenance of confidentiality of his PIN. In short, the cardholder finds himself in the witness box being cross-examined: a rather discomforting experience. (It is not too far-fetched to suggest that the prospect of such an experience may discourage prospective complainants from lodging reports of unexplained debits.) In short, the bank is a judge in its own cause: it decides whether to credit the cardholder's account for the loss suffered. There is no suggestion whatsoever that banks will not carry out this task judiciously and fairly. However, as justice should not only be done but should be seen to be done, the writer would prefer the setting up of an independent tribunal, comprising perhaps of representatives from the Association of Banks in Singapore, the Consumers' Association of Singapore and, possibly, the Monetary Authority of Singapore to decide on the question as to whether the bank should credit the cardholder's account with the missing funds. Although this may be a more time-consuming process, it is submitted that it would better satisfy the principles of natural

[10] In a police study conducted into the circumstances surrounding 28 ATM-related losses in the first seven months of 1985, the conclusion was reached that in most of the cases, the cardholder was at fault. In some cases, robbers and snatch thieves were to blame. Only in a few cases were unlawful withdrawals the result of mechanical fault. Several suggestions were made as to how illegal withdrawals could have occurred:

a. Ignorance: letting relatives and friends know the PIN;
b. Too trusting: letting a bystander help in using the machine. This happened mainly in the case of elderly or illiterate people;
c. Carelessness: writing the PIN down on paper and keeping it together with the card in one's wallet;
d. Impatience when the card is retained by the ATM: walking away when this happens after which the card emerges only to be taken by person next in the queue who then uses the card.

(Straits Times, 24 September 1985)

justice. In any case, the need for such enquiries would only arise infrequently.[11]

The position in the United States on this question is covered by the Electronic Fund Transfer Act 1978[12] (hereinafter referred to as the "EFTA") where the bank has to bear full liability for the loss unless it can prove that the withdrawal was an authorised one within the meaning of the Act.[13] If the bank fails to do this, it may nevertheless limit its liability if it is shown that the cardholder has failed to carry out certain actions relating to the reporting of his loss. Under this scheme, if the cardholder reports the loss or theft of his card within two business days, his maximum liability is US$50; the bank credits the cardholder's account with the balance of the loss. If the cardholder reports after two business days, he has to bear any loss that occurs following the close of the two business days after he discovers the loss or theft of his card but prior to giving notice to the bank, but in any case only up to a limit of US$500. If the cardholder notifies the bank after sixty days of receipt of the bank statement, the bank will not reimburse the cardholder with any loss which it establishes would not have occurred but for his failure to report within the sixty days. Certain prerequisites must be satisfied by the bank before it can limit its liability in the above manner.[14] In summary then, there is a graduated scheme of liability depending on when the consumer reports his loss.[15]

There are two conflicting decisions as regards the situation of a fraud committed on a cardholder, both of the Civil Court of the City of New York. In *Ognibene* v. *Citibank,*[16] the facts were that there were 2 ATMs, placed side by side with a customer service telephone in between them. The plaintiff was withdrawing US$20 from one of the machines when the perpetrator of the fraud, X pretending to use the telephone to complain about the malfunctioning of the other machine, asked whether he could use the plaintiff's card to test the purportedly malfunctioning machine. The trusting plaintiff handed his card over to X who used the card. Unknown to the plaintiff, X had noted the plaintiff's PIN when the plaintiff was using the other machine to withdraw the US$20. By "testing" the purportedly malfunctioning machine, X withdrew US$400 from the plaintiffs account.

[11] An example of such a committee comes from the insurance industry. The General Insurance Association of Singapore (GIA) has launched the Insurance Ombudsman Committee which comprises a lawyer, 2 GIA officials and one representative each from the Consumers Association of Singapore, the Singapore Society of Accountants and the Insurance Commissioner's Office of the Monetary Authority of Singapore. It settles disputes arising between policyholders and insurance companies. Its decision binds the insurance company but not the policyholder who might still seek legal redress.

[12] 15 U. S. C. A. Title 15, Chapter 41, Subchapter VI. See also Regulation E issued by the Board of Governors of the Federal Reserve System which implements the Act. Most of the provisions of the Act became effective on 10 May 1980. The sections that deal with consumer liability for unauthorised transfers (section 1693g) and the issuance of card, codes or other means of accessing an account (section 1693i) became effective on 8 February 1979..

[13] Section 1693g.

[14] The bank must show, first, that the card or other means of access utilised for the transfer was an accepted card or other means of access, and secondly, that the bank has provided a way which the user of the card or other means of access can be identified as the person who is authorised to use it, and thirdly, that it has disclosed to the consumer his liability for unauthorised electronic funds transfers and certain information pertaining to notification of the bank in the event the consumer believes that an authorised transfer has been or may be effected.

[15] This approach is also applicable to limiting consumer liability for unauthorised use of charge or credit cards following loss or theft of the card.

[16] 446 N. Y. S. 2d 845 (1981).

The court held that the plaintiff could recover his loss of $400 from the bank because the withdrawal was unauthorised within the meaning of the Act. To bring it within the meaning of an "unauthorised transfer", the plaintiff had first to put forward a *prima facie* case that (1) it was initiated by a person other than the cardholder and without his actual authority to initiate the transfer; (2) the cardholder had received no benefit from it; and (3) the cardholder did not furnish such person "with the card, code or other means of access" to his account.[17] The plaintiff succeeded in doing this. The Act then placed on the bank the burden of proving consumer liability for the transfer. To succeed in doing this, the bank had to prove that the transfer was authorised by rebutting the *prima facie* case. The bank argued that this was indeed the case because the plaintiff had voluntarily handed his card over to X and that therefore he had "furnished such persons with the card ... or other means of access" under limb (3) above. However, the court held that in order to invoke the limb successfully against the plaintiff, it must be shown that he had furnished both his card and his PIN to the third party, X. On the facts, the court held that he had not furnished his PIN to X. The bank's further attempt to limit its liability failed on the ground that the court was not satisfied "that the bank had disclosed to the consumer (cardholder) his liability for unauthorised electronic fund transfers and certain information pertaining to notification of the bank in the event the consumer believes that an unauthorised transfer has been or may be effected."[18] In *Feldman* v. *Citibank,*[19] where the facts were similar to those set out above, the court heard the testimony of the defendant bank's operational supervisor on the security processes used to insure against unauthorised use of an individual depositor's account. It then held, without reference to the EFTA, that "despite the plaintiffs testimony to the contrary, the facts of this case are such that taking into account the defendant's testimony as to the security provisions in effect, the court must make the inference that Mr. Feldman unwittingly allowed an unauthorised use of his account."[20] Judgment was then given in favour of the defendant bank.

A third decision, *Judd* v. *Citibank*[21] deals with the situation of an unexplained debit. In that case, the Civil Court of the City of New York, posited the issue as one of "evidence, burden and credibility".[22] Who is to be believed: the person or the machine? The cardholder had produced evidence that on the dates and times in question, she was at work and therefore could not have made the withdrawals. Her evidence was opposed by the defendant bank's computer printouts documenting the withdrawals in issue. In the event, the court held that, by a fair preponderance of credible evidence, the cardholder had proven that the withdrawals were erroneously charged to her account by the defendant bank.[23]

In the United Kingdom, there is some doubt as to the extent to which the Consumer Credit Act 1974 (hereinafter referred to as the

17 *Ibid.,* at p. 848.
18 *Ibid.*
19 443 N. Y. S. 2d 43 (1981).
20 Ibid., at p. 45. The Court referred to the report of the National Commission on Electronic Fund Transfers but not to the EFTA which was already in force.
21 435 N. Y. S. 2d 210 (1980).
22 *Ibid.,* at p. 211.
23 As in *Feldman* the Court referred to the report of the National Commission on Electronic Fund Transfer but not to the EFTA as the facts had taken place before the Act became operative.

"CCA")[24] covers debit cards, such as those which activate ATMs and EFTPOS transactions.[25] A credit cardholder is clearly protected by the CCA[26] which among other things, imposes a limit on the cardholder's liability in cases of fraud and theft,[27] requires card issuers to provide information on interest rates and to supply copies of the contract document,[28] imposes liabilities on card issuers where retailers default on their obligations to cardholders[29] and renders it an offence to proffer unsolicited cards.[30] In the case of debit cards, if these cards can additionally be used to obtain credit or secure an overdraft, or can be used in ATM machines of another bank, they would appear to fall within the meaning of "credit-token" under section 14. In such a case, when there is an unauthorised withdrawal, the cardholder cannot be made to bear more than £50 of the loss unless the person who used the card acquired possession of it with the cardholder's consent, in which case the cardholder bears the full loss.[31] In any case, the cardholder's liability ceases when he gives notice to the bank that the card has been lost or stolen.[32] In the case of dispute, such as where the cardholder alleges that use of the card was not authorised by him, the bank has first to prove that the card was lawfully supplied to the cardholder, and was

[24] The Act was passed on 31 July 1974 and was the product of nearly six years of concentrated efforts. The catalyst for reform was the work of the Crowther Committee on Consumer Credit which was appointed in 1968 and which published its report (Cmnd. 4596) in 1971.

[25] No legislation explicitly covers electronic funds transfer by debit cards. Although such cards do perform some of the functions of cheques, they do not, however, fall under the U. K. Bills of Exchange Act 1882. (See, for example, Ellinger, "Electronic Funds Transfers As A Deferred Settlement System", in *Electronic banking : The Legal Implications,* ed. Goode, 1985) In some respects, debit cards resemble cash as is the case in EFTPOS transactions; in other respects, they resemble credit cards, for example, both can give access to cash and can be used to acquire goods and services. Where overdraft facilities have been provided, they in fact can be used to obtain credit. Banks have become increasingly more creative in the integration of functions and services offered by debit and credit cards. For example, one local bank has introduced a card that combines some of these features: it carries the user's specimen signature, allows access to the bank's ATMs, can be used in EFTPOS transactions, enables the cardholder to obtain discounts at selected shops and restaurants, permits pre-arranged cash withdrawals at designated overseas branches, and the cardholder may apply for an overdraft. The cardholder also enjoys daily interest on his credit balance and can transfer funds through push-button telephones. Another bank has introduced a service whereby its credit cardholders can get cash advances from its ATM terminals, gain access to their savings and current accounts and pay for purchases at NETS terminals. The functional distinction between debit and credit cards has become increasingly blurred.

[26] It comes within the definition of a "credit-token" within section 14 of the Act. A credit-token is defined as a card, check, voucher, coupon, stamp, form, booklet or other document or thing given to an individual by a person carrying on a consumer credit business, who undertakes-

a. that on the production of it (whether or not some other action is also required) he will supply cash, goods and services (or any of them) on credit, or
b. that where, on the production of it to a third party (whether or not any other action is also required), the third party supplies cash, goods and services (or any of them), he will pay the third party for them (whether or not deducting any discount or commission), in return for payment to him by the individual.

Insofar as a debit card can be used to obtain credit as would be the case if it provides for an overdraft, or where the card may be used in an ATM machine owned by another bank, it would appear that such a card would come within the definition of a "credit-token".

[27] Sections 83 and 84 restrict the debtor's liability to £50 and exclude total liability for use of the credit-token after the creditor has been given notice that it is lost or stolen or is, for any reason, liable to misuse.

[28] Section 63 (4).

[29] Section 75.

[30] Section 51 (1).

[31] Sections 83 and 84(1).

[32] Section 84 (3).

accepted by him. It then has to prove further either that the use was so authorised, or that the use occurred before it received notice of the loss or theft of the card.[33]

The UNCITRAL Guide addresses these issues. Being in the form of a Guide, it advances arguments from both the bank's and cardholder's viewpoints, without being determinative. These viewpoints, however, are worthy of some reflection.

1) On the question of whether a "bank should be free from responsibility for error or delayed funds transfers caused by failures in computer hardware or software":

   "... On the one hand, it may be thought that technical problems of this nature are beyond the control of a bank and that the bank should be free from responsibility for any loss caused to customers (cardholders) as a result... On the other hand, it may be thought that the degree of computer reliability is such that they should be treated the same as any other type of equipment used by the banks ... As a result, a generalized exoneration from liability may be thought not to be justified but that exemption from liability for computer failure might be justified when the bank could not be expected to have prevented the failure or reduced its consequences."[34]

2) On the question of whether a "bank or the consumer (should) carry the burden of proof whether a debit to the transferor's (consumer's) account was authorised by him or occurred through his fault":

   "... It may be thought that it is unlikely that the record of the account to be debited could be in error as a result of undetected computer error or that a third person could fraudulently access the computer without the aid or the negligence of the customer that the burden of proof should properly rest upon the customer to show that the entry at the customer-activated terminal was made without his aid and was not the result of his negligence ... It may, however, be thought that fraudulent access to customer-activated terminals is a known and serious problem for which the banking industry should be responsible to its customers. It might even be thought that it is the duty of the banking industry to devise means of access to the computer through customer-activated terminals that are so secure that ordinary negligence on the part of the customer would not be sufficient to compromise them ..."[35]

3) On the question of whether there should be "a clearly articulated error resolution procedure":

   "... In some countries, it may be useful to prescribe by law the required error resolution procedures. It may be thought that, especially in regard to non-commercial accounts, mandatory error resolution procedures are an important measure of protection to bank customers who are otherwise in a weak position to argue with their bank about an alleged error on the

33 Section 171 (4).

34 Chapter on "Legal Issues Raised By Electronic Funds Transfers", Issue No. 19.

35 *Ibid,* Issue No. 21.

> part of the bank. However, it may also be thought that any error resolution procedure precribed by law would be apt to be either too general to be of much protection to bank customers or so detailed as to generate unnecessary expense. It may also be thought that in most countries, experience does not necessitate legislation on this point."[36]

In the United States and the United Kingdom, it is clear that the law favours the cardholder on both questions of liability and burden of proof. Legislative schemes have been introduced to aid the cardholder. Should similar schemes be introduced in Singapore? Obviously, there is no easy answer to this question. Whilst the UK and US schemes of liability may be overly-protective of the cardholder, the present position in Singapore which is preponderantly in favour of the bank is unsatisfactory. This submission is based on the following observations:

1) The bank is in a better position to bear any losses arising. It could accept these losses as part of business costs. Any business that is conducted for profit will have inherent risks. Perhaps, the necessary insurance coverage may be taken out. For the cardholder, a small sum in absolute terms may be a big sum relative to his total assets.
2) The cardholder may not know of the loss until some time later. After such a time lapse, he may not be able to recall important facts relating to the loss such as his whereabouts at the time of the debit, where his card had been kept at that time and whether he had entrusted anyone to draw funds from his account on his behalf. This time lapse is likely because the cardholder will only discover his loss in probably one of three ways: first, upon close examination of his bank account's monthly statement; secondly, on discovery that his card is missing (this happens only if the fraudulent user does not replace the card after its unauthorised use) and thirdly, in a system where no monthly statements are issued but a passbook is used, when he updates his passbook and discovers the unexplained debit on close examination. In the latter two situations, it is possible for there to be a considerable lapse between time of loss and time of discovery simply because the cardholder is neither contractually bound nor is it practically feasible for him to regularly check that his card is with him or that it has not been used in an unauthorised manner. He is also not required to present his passbook regularly for updating. Perhaps, the banks should consider the adoption of a common system which informs every cardholder on a regular basis of the withdrawal of funds from his account by electronic fund transfers (EFTS). Such information transmitted should also be clear and easily understood so that the cardholder can keep easy records of his expenditure.[37] This would be especially useful in the case of withdrawals from savings accounts which use passbooks for which no monthly statements are issued.[38] In the United States, a distinction is drawn between an account which may

[36] *Ibid.,* Issue No. 26.
[37] This is important so as to prevent the emergence of a reckless, free-spending society.
[38] In cheque banking, the cardholder is normally required by the terms of his agreement with the bank to check the monthly statement sent to him by the bank and to immediately report any discrepancies appearing.

be accessed by EFTs and one which only permits pre-authorised electronic fund transfers crediting the account, such as salaries paid through GIRO. In the former case, a periodic statement must be provided at least monthly for each monthly or shorter cycle in which an electronic fund transfer affecting the account has occurred, or every three months, whichever is more frequent.[39]

3) It is easier for the bank to prove that the cardholder was at fault than for the cardholder to prove that the bank was at fault.

However that may be, it is clear that in order to seek protection, the cardholder must satisfy any board of enquiry that his conduct as regards the safekeeping both of his card and confidentiality in his PIN cannot be impeached. Certain impositions should be exacted on the cardholder before he may benefit from any protection that is designed for him: for example, he should not be protected if it is shown that he had written his PIN on the card itself[40] or that he had made known this PIN to a third party in circumstances where fault may be attributed to him or that he had permitted a third party to withdraw funds on his behalf in unjustifiable circumstances.

(b) *What is the standard of care required of a cardholder with respect to the safekeeping of his card and the maintenance of confidentiality of his PIN?*

It is entirely possible for someone to obtain both possession of the card and knowledge of the PIN in circumstances falling short of actionable negligence on the part of the cardholder who may be a trusting, naive or forgetful person. As in the case of an action to render void a contract on the ground of *non est factum,* the question of whether the signatory or, in this case, the cardholder, has been negligent should be determined subjectively, that is, in accordance with the facts of the case taking into account the cardholder's infirmities and weaknesses, if any, and also the relationship between the cardholder and the fraudulent third party.[41] A loss may arise in a variety of circumstances: for example, a card may be stolen and used by someone who has previously observed its use and thereby knows the PIN; a withdrawal may have been effected by a third party under justifiable circumstances such as when a person is bedridden and, requiring funds urgently, requests a trusted friend or family member to make the withdrawal; a card and record of the PIN may be stolen from different parts of the cardholder's home or obtained under false pretences from a naive and trusting cardholder; a wallet or handbag containing both card and PIN written on a separate piece of paper but kept also in the wallet or handbag may be stolen or lost. In these circumstances, should the bank be permitted to pin full liability on the cardholder by relying on the clauses in the bank-cardholder contract which states that the

39 As to how the Privy Council has construed such a term, see *Tai Hing* v. *Liu Chong Hing Bank* [1985] 2 Lloyd's Rep 313, on appeal from the Court of Appeal of Hong Kong.

40 The position is less clear if the cardholder has written his PIN on a piece of paper which he then keeps in his wallet. If the card is also kept in his wallet which is then lost or stolen, thereby enabling a fraudulent third party to withdraw funds from his accounts, should the cardholder receive any protection? Not everyone has a good memory for numbers, especially as there may be other numbers to remember besides one's PIN such as one's identity card number, telephone numbers and recreation club numbers.

41 *Gallie* v. *Lee* [1971] A. C. 1004.

cardholder agrees not to reveal his PIN to any person under any circumstances, that the card will be used by him only, and that he shall accept full responsibility for all transactions made by the use or purported use of his card?

A comparison of the duties of a cardholder with those of a cheque-account holder (hereinafter referred to as a "customer") may be useful. The main duties owed by a customer to the bank are (a) to exercise reasonable care in drawing cheques so as not to mislead the bank or to facilitate forgery, and (b) to inform the bank when he discovers that cheques purported to be signed by him are in fact forged. In this regard, the Privy Council decision of *Tai Hing* v. *Liu Chong Hing Bank*[42] on appeal from the Court of Appeal of Hong Kong, is instructive. In that case, their Lordships reaffirmed the existence of the twin duties, as stated above, of customers to their banks. In the absence of express agreement, these duties would be implied in the bank-customer contract because they could be seen to be obviously necessary. For purposes of this discussion, it is noteworthy that they rejected the argument that customers have a wider duty to take such precautions as reasonable customers in their position would take to prevent forged cheques being presented to their banks for payment.

This decision indicates a judicial preference against extending the scope of the customer's duties towards his bank in the case of cheque banking. In particular, the words of Lord Scarman are instructive,[43]

> "One can fully understand the comment of Cons, J. A. that the banks must today look for protection. So be it. They can increase the severity of their terms of business, and they can use their influence, as they have in the past, to seek to persuade the legislature that they should be granted by statute further protection. But it does not follow that because they may need protection as their business expands the necessary incidents of their relationship with their customer must also change. The business of banking is the business not of the customer but of the bank. They offer a service, which is to honour their customer's cheques when drawn upon an account in credit or within an agreed overdraft limit. If they pay out upon cheques which are not his, they are acting outside their mandate and cannot plead his authority in justification of their debit to his account. This is a risk of the service which it is their business to offer."

This case may have some bearing on future developments in the bank-cardholder relationship.

(c) *What is the legal liability of the bank, if any, if the bank fails to make payment when instructed to do so?*

In the House of Lords decision of *London Joint Stock Bank v. Macmillan and Arthur,*[44] Lord Finlay L. C. described the banker-customer relationship as "one of debtor and creditor, with a superadded obligation on the part of the banker to honour the customer's cheques if the account is in credit." If the banker fails to honour a

[42] *Supra.,* n(39). See also Poh Chu Chai, "A Customer's Duty of Care Towards His Banker", [1986] 2 M. L. J. xxii.

[43] *Supra.,* n(39), at p. 321.

[44] [1918] A. C 777, at p. 789.

cheque without good cause, he will be liable for breach of contract and/or defamation. It is reasonable to expect the same relationship to exist between a cardholder and the bank with whom he has an EFTPOS or ATM arrangement. The bank therefore has a duty to honour the cardholder's payment instructions when there are sufficient funds.

However, it is not uncommon to find a clause in the bank-cardholder agreement stating that the cardholder will not hold the bank responsible should the bank fail to honour the card for any reason whatsoever. Naturally, the bank will argue that the clause will apply even if the cardholder has funds in his account but the card was not honoured due to bank error. Without expending too much effort, situations when this happens and its distressing effect on the cardholder can easily be imagined: a cardholder who finds himself at the head of a long queue at a supermarket is told, within hearing of other shoppers, that his card has not been honoured; a cardholder taking a prospective business client shopping and, having duly impressed his client with his selection of appropriate gifts for him, is told that his card has been "declined"; a tired but happy consumer having spent a considerable time shopping finds he cannot pay by EFTPOS and has to return all the carefully selected merchandise because he does not have sufficient cash. In these situations, the cardholder will probably suffer considerable embarrassment and mental distress for which damages for breach of contract are probably recoverable.[45] He may even be able to show pecuniary loss if the prospective client changes his mind on doing business with him. Alternatively, the cardholder may wish to consider an action in libel against the bank. In *Slim* v. *Stretch*,[46] Lord Atkin stated the test to be whether "the words or matter tend to lower the plaintiff in the estimation of right-thinking members of society generally." In the case of cheque banking, words such as "not sufficient", "present again" or "no account" used by the bank when a cheque is dishonoured have been held to be libellious.[47] On the other hand, the words "refer to drawer" have been held not to be libellious.[48] In the case of EFTPOS, when a card is not honoured, the terminal will respond with "No reply from bank". What then are the implications of these words? It is noted that the transaction may be unsuccessful for a variety of reasons. Besides lack of funds, other causes include computer shutdown or malfunction, or faulty communication links. The writer would suggest that the proper authorities, perhaps NETS, should widely publicise this fact so that no "right- thinking member of society" would cast negative imputations on a cardholder

45 See *Jarvis* v. *Swan Tours* [1973] 1 Q. B. 233, *Jackson* v. *Horizon Holidays Limited* [1975] 1 W. L. R. 1468 *Heywood* v. *Weller* [1976] 1 All E. R. 300 and *Cox* v. *Phillips Industries Limited* [1976] 1 W. L. R. 638.

46 [1936] 2 All E. R. 1237, at p. 1240.

47 For "not sufficient", see Hilbery J.'s judgment in *Davidson* v. *Barclays Bank Limited* [1940] All E. R. 316; for "present again", see *Baker* v. *Australia and New Zealand Bank* [1958] N. Z. L. R. 907, a decision of the Supreme Court of New Zealand; for "no account", see Sach J.'s judgment in *Wilson* v. *Midland Bank Limited,* an action tried at the Berkshire Assizes in Reading, for which refer to *The Reading Standard* for 13th October 1961.

48 See Scrutton J.'s judgment in *Flach* v. *London and South Western Bank* (1915) 31 T. L. R. 334.

whose card is rejected in public view.[49] Furthermore, notwithstanding the existence of the exemption clause mentioned earlier, when the above situations arise, the writer would urge banks to adopt a flexible approach and be prepared to compensate, perhaps on an *ex gratia* basis, a cardholder who can show that he has been greatly inconvenienced or embarassed or has suffered pecuniary loss.[50] Retail outlets offering EFTPOS facilities should also maintain "hotlines" to NETS and the banks to facilitate immediate enquiries on unsuccessful transactions. Cashiers should also be trained to handle these situations in a calm and restrained manner.

In the United States, the EFTA provides that "a financial institution shall be liable to a consumer for all damages proximately caused by *inter alia...* its failure to make an electronic fund transfer, in accordance with the terms and conditions of an account, in the correct amount or in a timely manner when properly instructed to do so by the consumer, except where-

1) the consumer's account had insufficient funds;
2) the funds were subject to legal process or other encumbrance restricting such transfer;
3) such transfer would exceed an established credit limit;
4) an electronic terminal has insufficient cash to complete the transaction;
5) as otherwise provided in regulations of the Federal Reserve Board.[51]

(d) *Is there a needfor legislation.*

The question whether a comprehensive *code* or statute on EFTs should be enacted has been debated in other jurisdictions as well.[52] An example of a comprehensive legislation is the EFTA which provides a "basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems."[53] The EFTA's purposes are declared in its preamble as follows:

1) "Congress finds that the use of electronic systems to transfer funds provides the potential for substantial benefits to

[49] In the Forum Page of the *Strait Times* of 8 and 16 July 1988, an exchange of letters took place between a reader calling himself INUTULIS and Mr. Lim Bak Wee, then General Manager of the company set up by the banks to run the EFTPOS system, NETS or Network for Electronic Transfers (S) Pte. Limited. INUTULIS had complained that his card had been rejected in public view. Mr. Lim clarified that "in that incident, there was a temporary disruption of service when the system encountered some technical problems. As a result the transaction could not be processed." He went on to explain that "when the "declined" appears it only means that [the] transaction could not be processed. Such a situation may arise from various reasons, one of which is due to the faulty communication links between NETS and the card issuing bank..." Such attempts to inform members of the public of the possible causes of the transaction being "declined" are welcomed.

[50] The cardholder may also wish to challenge the validity of the clause exempting the bank from liability as being unreasonable either at common law (*Levision* v. *Patent Steam Carpet Cleaning Company* [1978] Q. B. 69) or under the United Kingdom's Unfair Contract Terms Act. On the question of whether this Act is applicable in Singapore, see the writer's article, "Exemption Clauses & The Unfair Contract Terms Act: The Test of Reasonableness" [1985] 2 M. L. *J.* ccxxiv.

[51] Section 1693h.

[52] See for example, B. Crawford, "Does Canada Need A Payment Code" (1982-83) 7 Can. B. L. J. 44.

[53] Section 1693.

consumers. However, due to the unique characteristics of such systems, the application of existing consumer protection legislation is unclear, leaving the rights and liabilities of consumers, financial institutions, and intermediaries in electronic funds transfer undefined.

2) It is the purpose 9f this subchapter to provide a basic framework establishing the rights, liabilities and responsibilities of participants in electronic fund transfer systems. The primary objective of this subchapter, however, is the provision of individual consumer rights."

By way of summary and overall review, the EFTA provides for the following:

1) Full disclosure to the cardholder of the terms and conditions under which the bank provides EFT services, and changes in the terms to be similarly disclosed.[54]

2) The liability of a cardholder for unauthorised transfers to be limited to US$50 if notified within two days after discovery of the loss or theft of a card. This limit to be increased to US$500 if notice is given after two days and to be unlimited if unauthorised transfers are not reported within 60 days after the mailing of an account statement.[55]

3) Terminals operated by cardholders to be provided with means of giving written receipts for transactions for those cardholders who want them.[56]

4) Financial institutions to be given fixed time limits within which all unauthorised withdrawals notified less than sixty days after receipt of the statement must be investigated and regulated.[57]

5) Cardholders to be compensated by the bank should the unauthorised withdrawal be a result of computer malfunction or bank default.[58]

6) Setting out of model disclosure clauses for optional use by financial institutions to facilitate compliance with disclosure requirements and to aid cardholders in understanding the rights and responsibilities of participants in electronic fund transfers by utilising readily understandable languages.[59]

In Australia, the rights and liabilities of parties to an EFT are essentially contractual and are based on the common law. However, as a result of the increasing use of EFTs and the higher incidence of unauthorised withdrawals, pressure was exerted by consumer organisations on the Federal government to adopt a more active approach to reforms in this area of the law. A group called the Working Group Examining Consumer Protection Aspects of Electronic Funds Transfer Systems was set up to study the full implications of EFTs. The Australian Federation of Consumer Organisations (hereinafter referred to as "AFCO") as well as some of the state governments have been critical of the Federal government for its delay in acting to

54 Section 1693c.
55 Section 1693g.
56 Section 1693d.
57 Section 1693f.
58 Section 1693h.
59 Section 1693b.

regulate EFTs. AFCO had submitted a paper arguing for greater regulation to be effected as soon as possible.[60] These efforts have borne fruit. The Federal Government released its second report on the "Rights and Responsibilities of the Users and Providers of EFT Systems" in mid 1986. This Report, which has been endorsed by State Consumer Affairs Ministers, require that financial institutions a) provide information to customers on rights and obligations; b) improve receipt information; c) establish a A$50 maximum liability in cases of unauthorised use except where the customer has contributed to the unauthorised transactions; d) establish procedures for dispute resolution.

As mentioned earlier, the position in the United Kingdom is also largely based on the common law except where some provisions of the Consumer Credit Act 1974 are applicable.[61]

In Singapore, the writer submits that there should not be extensive regulation in this dynamic area of consumer law. This will hinder bank innovation and flexibility which are essential in order to meet new demands of consumers. However, the provision of some guidelines will be a step in the right direction. This will provide greater clarity and certainty which in turn will improve the trust and confidence between banks and cardholder. Although the existing situation is good, it could be better.[62] These guidelines should cover the matters discussed above. Solutions provided in the EFTA could be studied although they should not be adopted *verbatim.*

(e) *Is there a need to revise some of the current terms in the bank-cardholder contract?*

Current terms in the bank-cardholder contract weigh against the cardholder. These should be reviewed to ensure that they are more reasonable and balanced. The discussion above shows that in some respects the cardholder's position vis-a-vis the bank is somewhat uncertain. The clauses reinforces this inequality in the manner of their drafting. In practice, banks will act in a reasonable manner: for example, there is no doubt that banks will act honestly and fairly in their handling of disputes over unauthorised withdrawals. However, to promote general consumer confidence in the system, it is imperative that that which will be handled honestly and fairly must be seen clearly, at the outset, to be so. Better balanced clauses are therefore desirable. Such clauses will also help to instill and reinforce the element of good faith between banks and cardholders. After all, for many computer-illiterate cardholders, the onset of the computer age with its accompanying trail of new and sometimes bewildering linguistic twists and concepts can be quite intimidating.

Some ATM and EFTPOS agreement contain clauses that are widely drafted against the interests of cardholders. Besides those already mentioned earlier, other examples are clauses where cardholders may be required to notify the bank immediately of any loss,

[60] "Funny Money and Crazy Cards: The Case For Regulation of Electronic Funds Transfers Systems" (August 1985).
[61] *Supra.,* n(25-33).
[62] Examples of such guidelines are "Banking Services and the Consumer", section 5 on "New Technology" (1983) and "Losing At Cards: An investigation into consumers' problems with bank cash machines" (1985) both of which are published by the United Kingdom National Consumer Council.

theft or mutilation of the card without stating a corresponding duty on the part of banks to act on such notice; cardholders agree to accept full responsibility for all transactions made by the use of the card, even if made without their authority and are bound to accept the bank's records as binding, agreeing to waive all rights and remedies in respect of the use or purported use of the card without stating any possible bank liability for bank error or omission; the bank is given the right to cancel the use of the card at any time without notice to the cardholder or assigning any reason without at the same time stating that a cardholder also has such a corresponding right, and lastly, where the bank is given the right to vary any term of the contract at its absolute discretion without seeking the cardholder's consent or giving due notice to the cardholder. Having said this, the writer is pleased to note that some banks have recently redrafted the clauses in their ATM and EFTPOS agreements to reflect a better balance between their interests and those of the consumer.

The case of *Tai Hing* v. *Liu Chong Hing*,[63] once again has some relevance here. A further point arose in that case as to the effect of the following clauses:

> "A statement of the customer's account will be rendered once a month. Customers are desired: (1) to examine all entries in the statement of account and to report at once to the bank any error found therein. (2) to return the confirmation slip duly signed. In the absence of any objection to the statement within seven days after its receipt by the customer, the account shall be deemed to have been confirmed."
>
> "A monthly statement for each account will be sent by the bank to the depositor by post or messenger and the balance shown therein may be deemed to be correct by the bank if the depositor does not notify the bank in writing of any error therein within ten days after the sending of such statement..."
>
> "The bank's statement of my/our account will be confirmed by me/us without delay. In case of absence of such confirmation within a fortnight, the bank may take the said statement as approved by me/us."

Their Lordships held that "if banks wish to impose upon their customers an express obligation to examine their monthly statements and to make those statements, in the absence of query, unchallenge-able by the customer after expiry of a time limit, the burden of the obligation and of the sanction imposed must be brought home to the customer. In their Lordships' view, the provisions which they (the banks) have set out above do not meet this undoubtedly rigorous test ... Clear and unambiguous provision is needed."[64]

In the United Kingdom, the validity of these clauses are subject to the test of "reasonableness" under the Unfair Contract Terms Act 1977. In Singapore, there is some uncertainty as to whether the Act is applicable.[65]

Currently, customers in cheque banking transactions receive greater protection than cardholders in EFTs. For example, banks are

63 *Supra*., n(39).
64 *Ibid.*, at p. 323.
65 *Supra*., n(50).

liable if they pay on cheques that are forged or materially altered,[66] or if they dishonour cheques without good reasons, customers can countermand the payment of cheques by issuing a "stop payment notice" to the bank; customers are not bound by clauses in their agreement with the banks requiring them to report discrepancies in the statement of account within a stipulated time unless such clauses are clear and customers' attention is drawn specifically to them. As forms of payment systems, it is anomalous that consumers' legal rights may differ depending on which system they adopt for a particular transaction. Additionally, it is a known fact that banks will benefit from a "less-cash society" as operating costs will be reduced with less paperwork. Therefore, with the law favouring them even more in this new regime, it would appear that they would doubly benefit if some of the present inequities in the law between cardholder and bank arising from EFTs are not checked.

III. CONCLUSION

Clearly, the cooperation of all concerned parties is required to make the transition into a "less cash" society a smooth one. Understanding the problems each party faces will help a long way. Each party must play its part in the overall scheme of things. In particular, banks will have to continually upgrade their facilities with the following aspects in mind: personnel security, physical security, software security, communication security, education and training and sufficient liability coverage. They should always be conscious of the legitimate fears of consumers. Efforts should be made to allay these fears: one good starting point would be to reflect their own confidence in the system by redrafting clauses which may be found in ATM and EFTPOS agreements which foresee all kinds of losses to consumers and which place liability for such losses solely on them. Consumers on the other hand should seek to understand the workings of the various EFT systems, get to know how frauds may be perpetrated and, more importantly, find out how they can prevent these frauds from occurring. In the case of EFTPOS, retailers and merchants should render the necessary cooperation to NETS and the banks to make EFTPOS facilities more readily available, thereby maximising the convenience cashless living affords the consumer. Cashiers should be trained in the efficient handling of EFTPOS terminals. They should also be clearly briefed on the necessary action to be taken in the event of computer malfunction or breakdown. Practical tips on how to handle irate customers will also be useful.

HO PENG KEE*

In the case of material alteration, the bank can escape liability by showing that the customer has in some way been negligent in the way in which he drew up the order so that a third party was able to alter the mandate without detection. See Poh Chu Chai *supra.*, n(42).

* LL. B. (Sing.), LL. M. (Harv.), Advocate and Solicitor, Supreme Court of Singapore, Senior Lecturer, Faculty of Law, National University of Singapore.